The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
07/12/2016

SUBJECT:
Cumulative Security Update for Microsoft Edge (MS16-085)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Edge that could allow for remote code execution. Microsoft Edge replaced Internet Explorer as the default browser on Windows 10. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Windows 10
- Windows 10 (Version 1511)

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft Edge that could allow for remote code execution. Details of these vulnerabilities are as follows:

- A Security Feature Bypass exists when Microsoft Edge does not properly implement Address Space Layout Randomization (ASLR). (CVE-2016-3244)
- Two Memory Corruption Vulnerabilities exists when Microsoft Edge improperly accesses objects in memory. (CVE-2016-3246, CVE-2016-3264)

- Five Scripting Engine Memory Corruption Vulnerabilities exist in the way that the Chakra JavaScript engine renders when handling objects in memory in Microsoft Edge. (CVE-2016-3248, CVE-2016-3259, CVE-2016-3260, CVE-2016-3265, CVE-2016-3269)
- A Scripting Engine Information Disclosure Vulnerability exists when VBScript improperly discloses the contents of its memory, which could provide an attacker with information to further compromise the user's computer or data. (CVE-2016-3271)
- A Microsoft Browser Information Disclosure Vulnerability exists when the Microsoft Browser XSS Filter does not properly validate content under specific conditions. (CVE-2016-3273)
- A Microsoft Browser Spoofing Vulnerability exists when a Microsoft browser does not properly parse HTTP content. (CVE-2016-3274)
- A Microsoft Browser Spoofing Vulnerability exists when the Microsoft Browser in reader mode does not properly parse HTML content. (CVE-2016-3276)
- A Microsoft Browser Information Disclosure Vulnerability exists when the Microsoft Browser improperly handles objects in memory. (CVE-2016-3277)

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/library/security/ms16-085

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3244
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3246
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3248
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3259
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3260
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3264
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3265
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3269
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3271
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3273
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3274
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3276
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3277